

On conjugacy classes of subgroups of the general linear group and cyclic orbit codes

Felice Manganiello, Anna–Lena Trautmann and Joachim Rosenthal

Institute of Mathematics
University of Zurich
Winterthurerstrasse 190
CH-8057 Zurich, Switzerland
www.math.uzh.ch/aa

Abstract—Orbit codes are a family of codes applicable for communications on a random linear network coding channel. The paper focuses on the classification of these codes. We start by classifying the conjugacy classes of cyclic subgroups of the general linear group. As a result, we are able to focus the study of cyclic orbit codes to a restricted family of them.

INTRODUCTION

The interest on constructions of codes for random linear network coding arises with the paper [1]. This paper introduces the notion of a code as a subset of $\mathcal{P}(\mathcal{V})$, that is the set of all subspaces of a vector space over a finite field \mathbb{F}_q . This set is equipped with a metric, suitable for the model of communication introduced, called subspace distance, defined as follows: for every $\mathcal{U}_1, \mathcal{U}_2 \in \mathcal{P}(\mathcal{V})$,

$$d(\mathcal{U}_1, \mathcal{U}_2) = \dim(\mathcal{U}_1) + \dim(\mathcal{U}_2) - 2\dim(\mathcal{U}_1 \cap \mathcal{U}_2).$$

The set of all subspaces of dimension k is called the Grassmannian and denoted by $\mathcal{G}_{\mathbb{F}_q}(k, n)$.

Some effort has been done in the direction of constructing codes for random linear network coding in the last few years. Some results can be found in [1], [2], [3], [4], [5], [6].

In order to introduce orbit codes, we first recall the notion of the right action of the group $GL_n(\mathbb{F}_q)$ of the invertible matrices on the Grassmannian.

Definition 1: Let $\mathcal{U} \in \mathcal{G}_{\mathbb{F}_q}(k, n)$ and $U \in \mathbb{F}_q^{k \times n}$ a matrix such that $\mathcal{U} := \text{rowsp}(U)$. We define the following operation

$$\mathcal{U}A := \text{rowsp}(UA).$$

As a consequence we obtain the following right action of $GL_n(\mathbb{F}_q)$ on $\mathcal{G}_{\mathbb{F}_q}(k, n)$

$$\begin{aligned} \mathcal{G}_{\mathbb{F}_q}(k, n) \times GL_n(\mathbb{F}_q) &\rightarrow \mathcal{G}_{\mathbb{F}_q}(k, n) \\ (\mathcal{U}, A) &\mapsto \mathcal{U}A. \end{aligned}$$

The action just defined on $\mathcal{G}_{\mathbb{F}_q}(k, n)$ is independent of the choice of the representation matrix $U \in \mathbb{F}_q^{k \times n}$ it is distance preserving. For more information the reader is referred to [6].

Orbit codes are a certain class of constant dimension codes.

The authors were partially supported by Swiss National Science Foundation under Grant no. 126948.

Definition 2 ([6]): Let $\mathcal{U} \in \mathcal{G}_{\mathbb{F}_q}(k, n)$ and $\mathfrak{S} < GL_n(\mathbb{F}_q)$ a subgroup. Then

$$\mathcal{C} = \{\mathcal{U}A \mid A \in \mathfrak{S}\}$$

is called orbit code. An orbit code is called cyclic if there exists a subgroup defining it that is cyclic.

In [6] the authors show that orbit codes satisfy properties that are similar to the ones of linear codes for classical coding theory. Moreover, some already known constructions, such as the ones contained in [1] and [2], are actually orbit codes.

This paper focuses on the classification of orbit codes. In order to do so, we are going to give a classification of the conjugacy classes of subgroups of $GL_n(\mathbb{F}_q)$.

The paper is structured as follows. The first section is dedicated to the classification of subgroups of $GL_n(\mathbb{F}_q)$. More in detail, we are able to characterize the properties of a unique representative for the conjugacy classes of cyclic subgroups of $GL_n(\mathbb{F}_q)$. The result is contained in Theorem 10. With some examples we also show that the classification as it is cannot be extended to arbitrary subgroups. In the second section we apply these results to cyclic orbit codes. The main result is that we can focus on the study of cyclic orbit codes defined by a cyclic group generated by a matrix in rational canonical form. Moreover we study the construction of codes in this case and relate them to completely reducible cyclic orbit codes. At last we give some conclusions.

I. CHARACTERIZATION OF CYCLIC SUBGROUPS OF $GL_n(\mathbb{F}_q)$

In this section we investigate the cyclic subgroups of $GL_n(\mathbb{F}_q)$. The goal is to characterize them in a way that is suitable for the construction of orbit codes. More specifically we are interested in answering the question about when two cyclic groups are conjugate to each other.

Consider $GL_n(\mathbb{F}_q)$ and the following equivalence relation on it: Given $A, B \in GL_n(\mathbb{F}_q)$ then

$$A \sim_c B \iff \exists L \in GL_n(\mathbb{F}_q) : A = L^{-1}BL.$$

A natural choice of representatives of the classes of $GL_n(\mathbb{F}_q)/\sim_c$ is given by the *rational canonical form*. Rational canonical forms are based on companion matrices, whose definition is as follows.

Definition 3: Let $p = \sum_{i=0}^s p_i x^i \in \mathbb{F}_q[x]$ be a monic polynomial. Its companion matrix is the matrix

$$M_p := \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & 0 & 0 & & 1 \\ -p_0 & -p_1 & -p_2 & \cdots & -p_{s-1} \end{pmatrix} \in \mathbb{F}_q^{s \times s}.$$

The following theorem states the existence and uniqueness of a rational canonical form.

Theorem 4 ([7, Chapter 6.7]): Let $A \in GL_n(\mathbb{F}_q)$. Then there exists a matrix $L \in GL_n(\mathbb{F}_q)$ such that

$$L^{-1}AL = \text{diag}(M_{p_1^{e_{11}}}, \dots, M_{p_1^{e_{1r_1}}}, \dots, M_{p_m^{e_{m1}}}, \dots, M_{p_m^{e_{mr_m}}}) \quad (1)$$

is a block diagonal matrix where $p_i \in \mathbb{F}_q[x]$ are irreducible polynomials, $e_{ij} \in \mathbb{N}$ are such that $e_{i1} \geq \dots \geq e_{ir_i}$, $\chi_A = \prod_{i,j} p_i^{e_{ij}}$ and $\mu_A = \prod_i p_i^{e_{i1}}$ represent respectively the characteristic and the minimal polynomials of A and $M_{p_i^{e_{ij}}}$ denotes the companion matrix of the polynomial $p_i^{e_{ij}}$. Moreover, the matrix (1) is unique for any choice of $A \in GL_n(\mathbb{F}_q)$.

Definition 5: Let $A \in GL_n(\mathbb{F}_q)$. The matrix (1) is called rational canonical form of A and the polynomials $p_1^{e_{11}}, \dots, p_1^{e_{1r_1}}, \dots, p_m^{e_{m1}}, \dots, p_m^{e_{mr_m}} \in \mathbb{F}_q[x]$ are its elementary divisors.

The following lemma motivates why rational canonical forms are a good choice of representatives for the classes of $GL_n(\mathbb{F}_q)/\sim_c$.

Lemma 6: Let $A, B \in GL_n(\mathbb{F}_q)$. Then the following statements are equivalent:

- 1) $A \sim_c B$, and
- 2) A and B have the same rational canonical form.

This lemma is well-known and is a direct consequence of the uniqueness of the rational canonical form.

Now we want to extend the previous characterization to subgroups of $GL_n(\mathbb{F}_q)$.

Consider the set of all subgroups of $GL_n(\mathbb{F}_q)$

$$\mathbf{G} := \{\mathfrak{S} \mid \mathfrak{S} < GL_n(\mathbb{F}_q)\}$$

and the following equivalence relation on it. Given $\mathfrak{S}_1, \mathfrak{S}_2 \in \mathbf{G}$ then

$$\mathfrak{S}_1 \sim_c \mathfrak{S}_2 \iff \exists L \in GL_n(\mathbb{F}_q) : \mathfrak{S}_1 = L^{-1}\mathfrak{S}_2L.$$

The following theorem extends the arguments of Lemma 6 to the case of cyclic subgroups.

Theorem 7: Let $A, B \in GL_n(\mathbb{F}_q)$ and $\mathfrak{S}_A = \langle A \rangle, \mathfrak{S}_B = \langle B \rangle < GL_n(\mathbb{F}_q)$ be the two cyclic groups generated by them. Then, $\mathfrak{S}_A \sim_c \mathfrak{S}_B$ if and only if $|\mathfrak{S}_A| = |\mathfrak{S}_B|$ and there exists an $i \in \mathbb{N}$ with $\gcd(i, |\mathfrak{S}_B|) = 1$ such that $A \sim_c B^i$.

Proof:

\Rightarrow Since $\mathfrak{S}_A \sim_c \mathfrak{S}_B$, it follows that there exists an $L \in GL_n(\mathbb{F}_q)$ such that $\mathfrak{S}_A = L^{-1}\mathfrak{S}_BL$, implying

that the two groups have the same order. Moreover, it follows that the group homomorphism

$$\begin{aligned} \varphi : \mathfrak{S}_A &\rightarrow GL_n(\mathbb{F}_q) \\ A^i &\mapsto LA^iL^{-1} \end{aligned}$$

is an isomorphism if restricted to the image of φ . As a consequence, the generator A of \mathfrak{S}_A is mapped to a generator of $L\mathfrak{S}_AL^{-1} = \mathfrak{S}_B$, i.e., an element of $\{B^i \mid \gcd(i, |\mathfrak{S}_B|) = 1\}$. Then, there exists an $i \in \mathbb{N}$ with $\gcd(i, |\mathfrak{S}_B|) = 1$ such that $LAL^{-1} = B^i$, which implies that $A \sim_c B^i$.

\Leftarrow From the hypothesis we know that $\langle B^i \rangle = \mathfrak{S}_B$ and that there exists $L \in GL_n(\mathbb{F}_q)$ such that $A = L^{-1}B^iL$. The statement follows as a consequence. \blacksquare

We introduce the following definition.

Definition 8 ([8, Definition 3.2]): Let $p \in \mathbb{F}_q[x]$ be a nonzero polynomial. If $p(0) \neq 0$, then the least integer $e \in \mathbb{N}$ such that p divides $x^e - 1$ is called the order of p .

The definition is generalizable to any $p \in \mathbb{F}_q[x]$ but it is not interesting for the purpose of this paper since we will only consider irreducible polynomials.

In order to give unique representatives for the classes of cyclic groups contained in \mathbf{G}/\sim_c we need the following lemma.

Lemma 9: Let $A \in GL_n(\mathbb{F}_q)$, $p_{A,1}^{e_{A,1}}, \dots, p_{A,m}^{e_{A,m}} \in \mathbb{F}_q[x]$ its elementary divisors, where $p_{A,j}$ for $j \in \{1, \dots, m\}$ are not necessarily distinct, and $\mathfrak{S}_A < GL_n(\mathbb{F}_q)$ the cyclic group generated by A . Then, for every $i \in \mathbb{N}$ with $\gcd(i, |\mathfrak{S}_A|) = 1$, the elementary divisors of A^i are exactly m many. If we denote them by $p_{A^i,1}^{e_{A^i,1}}, \dots, p_{A^i,m}^{e_{A^i,m}} \in \mathbb{F}_q[x]$, then, up to reordering, the order of $p_{A,j}$ is the same as the one of $p_{A^i,j}$ and $e_{A,j} = e_{A^i,j}$ for $j = 1, \dots, m$.

Proof: First we prove the case where the elementary divisor is unique. At the end of the proof we will give the main remark that implies the generalized statement.

Let $p_A^{e_A} \in \mathbb{F}_q[x]$ be the elementary divisor of a matrix $A \in GL_n(\mathbb{F}_q)$ and $k := n/e_A$. Let $\mathbb{F}_{q^k} := \mathbb{F}_q[x]/(p_A)$ be the splitting field of the polynomial p_A and $\mu \in \mathbb{F}_{q^k}$ a primitive element of it. There exists a $j \in \mathbb{N}$ such that $p_A = \prod_{u=0}^{k-1} (x - \mu^{jq^u})$. Since $p_A^{e_A}$ is the unique elementary divisor of the matrix A , it corresponds to the characteristic and the minimal polynomial of A . As a consequence we obtain that the Jordan normal form of A over \mathbb{F}_{q^k} is

$$J_A = \text{diag} \left(J_{A, \mu^j}^{e_A}, \dots, J_{A, \mu^{jq^{k-1}}}^{e_A} \right)$$

where $J_{A, \mu^{jq^u}}^{e_A} \in GL_{e_A}(\mathbb{F}_{q^k})$ is a unique Jordan block with diagonal entries μ^{jq^u} for $u = 0, \dots, k-1$.

By the Jordan normal form of A it follows that for every $i \in \mathbb{N}$ the characteristic polynomial of A^i is $p_{A^i} = (\prod_{u=0}^{k-1} (x - \mu^{ijq^u}))^{e_A}$. Let us now focus on the i 's such that $\gcd(i, |\mathfrak{S}_A|) = 1$. A^i is then a generator of \mathfrak{S}_A , i.e., $p_{A^i} \in \mathbb{F}_q[x]$ is a monic irreducible polynomial whose order is the same as the one of p_A .

In order to conclude that $p_{A^i}^{e_A}$ is the elementary divisor of A^i we consider its rational canonical form. Assume that the elementary divisors of A^i were more than one. Without loss of generality we can consider them to be two, i.e., $p_{A^i}^{e_{A,1}}$ and $p_{A^i}^{e_{A,2}}$. This means that its rational canonical form is $\text{RCF}(A^i) = \text{diag}(M_{p_{A^i}^{e_{A,1}}}, M_{p_{A^i}^{e_{A,2}}})$ where we use the operator RCF as an abbreviation for rational canonical form and $e_A = e_{A,1} + e_{A,2}$. For any $j \in \mathbb{N}$ we obtain that the matrix $\text{RCF}((\text{RCF}(A^i))^j)$ is a block diagonal matrix with at least two blocks. Let $j \in \mathbb{N}$ such that $ij \equiv 1 \pmod{|\mathfrak{S}_A|}$ and $L \in GL_n(\mathbb{F}_q)$ be a matrix such that $\text{RCF}(A^i) = L^{-1}A^iL$, then

$$(\text{RCF}(A^i))^j = (L^{-1}A^iL)^j = L^{-1}AL \sim_c A$$

implying that

$$\text{RCF}(A) = \text{RCF}((\text{RCF}(A^i))^j)$$

This leads to a contradiction since $\text{RCF}(A) = M_{p_A^{e_A}}$ has only one block. We conclude that $p_{A^i}^{e_A}$ is the elementary divisor of A^i .

The only difference in the case where $m > 1$ consists in the choice of the splitting field. Given $p_{A,1}^{e_{A,1}}, \dots, p_{A,m}^{e_{A,m}} \in \mathbb{F}_q[x]$ the elementary divisors of A and $p_{A,l_1}, \dots, p_{A,l_r}$ with $l_1, \dots, l_r \in \{1, \dots, m\}$ the maximal choice distinct polynomials from the elementary divisors, the splitting field on which the proof is based is $\mathbb{F}_q[x]/(\prod_{t=1}^r p_{A,l_t})$. ■

We are now ready to characterize cyclic subgroups of $GL_n(\mathbb{F}_q)$ via the equivalence relation \sim_c based only on their elementary divisors.

Theorem 10: Let $A, B \in GL_n(\mathbb{F}_q)$ and $\mathfrak{S}_A, \mathfrak{S}_B \in \mathbf{G}$ the cyclic subgroups generated by them. Then, $\mathfrak{S}_A \sim_c \mathfrak{S}_B$ if and only if the following conditions hold:

- 1) A and B have the same number of elementary divisors, and
- 2) if $p_{A,1}^{e_{A,1}}, \dots, p_{A,m}^{e_{A,m}} \in \mathbb{F}_q[x]$ and $p_{B,1}^{e_{B,1}}, \dots, p_{B,m}^{e_{B,m}} \in \mathbb{F}_q[x]$ are the elementary divisors of respectively A and B , then, up to a reordering argument, the orders of $p_{A,j}$ and $p_{B,j}$ are the same and $e_{A,j} = e_{B,j}$ for $j = 1, \dots, m$.

Proof:

⇒ By Theorem 7, there exists a power $i \in \mathbb{N}$ with $\gcd(i, |\mathfrak{S}_A|) = 1$ such that $A \sim_c B^i$, i.e., they have the same elementary divisors. The statement follows with Lemma 9.

⇐ Let $p_{B,l_1}, \dots, p_{B,l_r} \in \mathbb{F}_q[x]$ with $l_1, \dots, l_r \in \{1, \dots, m\}$ be the maximal choice of pairwise coprime polynomials from the elementary divisors of B , \mathbb{F} the splitting field of $\prod_{t=1}^r p_{B,l_t}$ and $\mu \in \mathbb{F}$ a primitive element of it. Consider the notation $k_j := \deg p_{B,l_j}$ for $j = 1, \dots, r$. Then, there exist $i_{B,1}, \dots, i_{B,r} \in \mathbb{N}$ such that $p_{B,l_j} = \prod_{u=0}^{k_j-1} (x - \mu^{i_{B,j}q^u})$ for $j = 1, \dots, r$. The same holds for the matrix A , i.e., there exist $i_{A,1}, \dots, i_{A,r} \in \mathbb{N}$ such that $p_{A,l_j} = \prod_{u=0}^{k_j-1} (x - \mu^{i_{A,j}q^u})$ for $j = 1, \dots, r$. By the condition on the orders, there exists a unique $i \in \mathbb{N}$ such that $i_{A,j} \equiv i \cdot i_{B,j} \pmod{\text{ord}(p_{B,l_j})}$ for

$j = 1, \dots, r$. It follows that the elementary divisors of B^i and the ones of A are the same, i.e., $A \sim_c B^i$. ■

The theorem states that we can uniquely represent the classes of cyclic subgroups in \mathbf{G}/\sim_c by considering the cyclic subgroups generated by a rational canonical form based on the choice of a sequence of polynomials of the type $p_1^{e_1}, \dots, p_m^{e_m} \in \mathbb{F}_q[x]$ where the polynomials p_1, \dots, p_m are irreducible and $\sum_{j=1}^m e_j \cdot \deg(p_j) = n$. Moreover, what matters in the choice of the polynomials p_j 's is only their degrees and orders.

Trivially, the following holds for the cardinality of a cyclic group.

Corollary 11: Let $\mathfrak{S}_A = \langle A \rangle < GL_n(\mathbb{F}_q)$. Then the order of \mathfrak{S}_A is the least common multiple of the orders of the elementary divisors $p_1^{e_1}, \dots, p_m^{e_m} \in \mathbb{F}_q[x]$ of the matrix A .

To conclude the section we are going to give an example explaining why a straight forward generalization of Theorem 10 to any subgroup of $GL_n(\mathbb{F}_q)$ does not work.

Example 12:

- 1) Consider the following matrix over \mathbb{F}_2 :

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

Although the elementary divisor of A and the one of its transpose A^t is the same, the groups $\mathfrak{S}_A = \langle A \rangle = \langle A, A \rangle$ and $GL_3(\mathbb{F}_2) = \langle A, A^t \rangle$ are not conjugate.

- 2) Let $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2 + x + 1)$ and $\mu \in \mathbb{F}_4$ a primitive element. Consider the following matrices over \mathbb{F}_4 :

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, B_1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix},$$

$$\text{and } B_2 = \begin{pmatrix} \mu+1 & 1 & \mu \\ \mu & \mu & \mu+1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Although $B_1 \sim_c B_2$, i.e., they have the same unique elementary divisor, it holds that $|\langle A, B_1 \rangle| \neq |\langle A, B_2 \rangle|$, meaning that the two groups are not conjugate.

II. CONJUGATE GROUPS AND CYCLIC ORBIT CODES

We now apply the results from the previous section to the characterization of cyclic codes.

Definition 13: Let $\mathfrak{S}_1, \mathfrak{S}_2 < GL_n(\mathbb{F}_q)$ and $\mathcal{C}_1 := \{\mathcal{U}_1 A \mid A \in \mathfrak{S}_1\}, \mathcal{C}_2 := \{\mathcal{U}_2 A \mid A \in \mathfrak{S}_2\} \subseteq \mathcal{G}_{\mathbb{F}_q}(k, n)$ be two orbit codes. We say that \mathcal{C}_1 and \mathcal{C}_2 are conjugate or simply $\mathcal{C}_1 \sim_c \mathcal{C}_2$ if there exists a matrix $L \in GL_n(\mathbb{F}_q)$ such that

$$\mathcal{U}_2 = \mathcal{U}_1 L \text{ and } \mathfrak{S}_2 = L^{-1} \mathfrak{S}_1 L,$$

i.e., $\mathcal{C}_2 = \{\mathcal{U}_1 AL \mid A \in \mathfrak{S}_1\} = \{\mathcal{U}_1 L(L^{-1}AL) \mid A \in \mathfrak{S}_1\}$.

In order to further study properties of orbit codes, we need to introduce the notion of distance distribution for orbit codes. Due to [6], we are able to adapt the definition of weight enumerator from classical coding theory to orbit codes. But first we recall some facts from [6].

Definition 14 ([6, Definition 3]): Let $\mathcal{U} \in \mathcal{G}_{\mathbb{F}_q}(k, n)$. Then the stabilizer group of \mathcal{U} is defined as

$$\text{Stab}(\mathcal{U}) := \{A \in GL_n(\mathbb{F}_q) \mid \mathcal{U}A = \mathcal{U}\} < GL_n(\mathbb{F}_q).$$

The following proposition is important in order to define the distance distribution.

Proposition 15 ([6, Proposition 8]): Let $\mathcal{C} = \{\mathcal{U}A \mid A \in \mathfrak{S} < GL_n(\mathbb{F}_q)\}$ be an orbit code. Then it holds that

$$|\mathcal{C}| = \frac{|\mathfrak{S}|}{|\mathfrak{S} \cap \text{Stab}(\mathcal{U})|}$$

and

$$d(\mathcal{C}) = \min_{A \in \mathfrak{S} \setminus \text{Stab}(\mathcal{U})} d(\mathcal{U}, \mathcal{U}A).$$

Definition 16: Let $\mathcal{C} = \{\mathcal{U}A \mid A \in \mathfrak{S} < GL_n(\mathbb{F}_q)\} \subseteq \mathcal{G}_{\mathbb{F}_q}(k, n)$ be an orbit code. The distance distribution of \mathcal{C} is the tuple $(D_0, \dots, D_k) \in \mathbb{N}^{k+1}$ such that

$$D_i := \frac{|\{A \in \mathfrak{S} \mid d(\mathcal{U}, \mathcal{U}A) = 2i\}|}{|\mathfrak{S} \cap \text{Stab}(\mathcal{U})|}.$$

As a consequence we obtain that $D_0 = 1$ and $\sum_{i=0}^k D_i = |\mathcal{C}|$. We are able to state the following theorem that characterizes conjugate orbit codes and that is a generalization of Theorem 9 from [9].

Theorem 17: The binary relation \sim_c on orbit codes is an equivalence relation. Moreover, let $\mathcal{C}_1, \mathcal{C}_2$ be two orbit codes such that $\mathcal{C}_1 \sim_c \mathcal{C}_2$, then $|\mathcal{C}_1| = |\mathcal{C}_2|$ and they have the same distance distribution.

Proof: The fact that \sim_c is an equivalence relation on orbit codes is a consequence of Theorem 7.

Let $\mathcal{C}_1 := \{\mathcal{U}A \mid A \in \mathfrak{S} < GL_n(\mathbb{F}_q)\}$ and $L \in GL_n(\mathbb{F}_q)$ such that $\mathcal{C}_2 = \{\mathcal{U}AL \mid A \in \mathfrak{S}\}$. The same cardinality is consequence of the fact that given $A, B \in \mathfrak{S}$ then

$$\mathcal{U}AL = \mathcal{U}BL \iff \mathcal{U}A = \mathcal{U}B.$$

The same distance distribution follows from the distance preserving property of the $GL_n(\mathbb{F}_q)$ action on $\mathcal{G}_{\mathbb{F}_q}(k, n)$, i.e., $d(\mathcal{U}L, \mathcal{U}AL) = d(\mathcal{U}, \mathcal{U}A)$. ■

The importance of this last theorem is that two conjugate orbit codes are not distinguishable from the point of view of cardinality and distance distribution. Theorem 10 translates as follows in the language of orbit codes.

Corollary 18: Every cyclic orbit code is conjugate to a cyclic orbit code defined by a cyclic group generated by a matrix in rational canonical form.

This fact gives us the opportunity to consider only cyclic orbit codes out of matrices in rational canonical form for the study of codes with good parameters.

We are now interested in these orbits codes.

Theorem 19: Let $M := \text{diag}(M_{p_1^{e_1}}, \dots, M_{p_t^{e_t}}) \in GL_n(\mathbb{F}_q)$ a matrix such that $p_i \in \mathbb{F}_q[x]$ are monic irreducible polynomials and $d_i := \deg(p_i^{e_i})$ for $i = 1, \dots, t$. Let $\mathcal{U} = \text{rowsp}(U_1, \dots, U_t) \in \mathcal{G}_{\mathbb{F}_q}(k, n)$ with $U_i \in \mathbb{F}_q^{k \times d_i}$ and where (U_1, \dots, U_t) is in row reduced echelon form. For any $i \in \{1, \dots, t\}$, let \bar{U}_i be a submatrix of U_i as depicted in Figure 1.

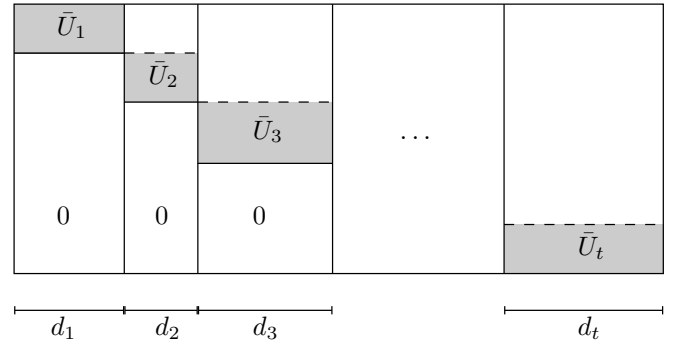


Fig. 1. The matrix U in row reduced echelon form.

If $\mathcal{C} := \{\mathcal{U}M^i \mid i \in \mathbb{N}\}$ and $\mathcal{C}_i := \{\text{rowsp}(\bar{U}_i)M_{p_i^{e_i}}^j \mid j \in \mathbb{N}\}$, then

$$d(\mathcal{C}) \geq 2k - 2 \sum_{i=1}^t \max_{j \in \mathbb{N}} \dim(\text{rowsp}(\bar{U}_i) \cap \text{rowsp}(\bar{U}_i M_{p_i^{e_i}}^j)), \quad (2)$$

and $|\mathcal{C}| := \text{lcm}(|\mathcal{C}_1|, \dots, |\mathcal{C}_t|)$.

Proof: Consider the following projections

$$\pi_i : \begin{array}{ccc} \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^{d_i} \\ (v_1, \dots, v_n) & \longmapsto & (v_{l_{i-1}+1}, \dots, v_{l_i}) \end{array}$$

where $l_i = \sum_{j=1}^i d_j$ for $i = 1, \dots, t$. Since (U_1, \dots, U_t) has full rank and is in row reduced echelon form, the matrices \bar{U}_i have full rank. Let $\bar{\mathcal{U}}_i \subset \mathbb{F}_q^n$ be the space spanned by the rows of (U_1, \dots, U_t) indexed by the rows corresponding to \bar{U}_i . Since \bar{U}_i has full rank it follows that $\pi_i|_{\bar{\mathcal{U}}_i}$ is injective for $i = 1, \dots, t$. As a consequence we obtain that for any $i = 1, \dots, t$, if we define $m_i \in \mathbb{N}$ such that

$$\dim(\bar{\mathcal{U}}_i \cap \bar{\mathcal{U}}_i M_{p_i^{e_i}}^{m_i}) \geq \dim(\bar{\mathcal{U}}_i \cap \bar{\mathcal{U}}_i M_{p_i^{e_i}}^j), \quad \forall j \in \mathbb{N}$$

and $\mathcal{V}_i := \bar{\mathcal{U}}_i \cap \bar{\mathcal{U}}_i M_{p_i^{e_i}}^{m_i}$, then

$$\pi_i(\mathcal{V}_i) \subseteq \text{rowsp}(\bar{U}_i) \cap \text{rowsp}(\bar{U}_i M_{p_i^{e_i}}^{m_i}).$$

It follows that

$$\dim(\mathcal{V}_i) \leq \max_{j \in \mathbb{N}} \dim(\text{rowsp}(\bar{U}_i) \cap \text{rowsp}(\bar{U}_i M_{p_i^{e_i}}^j)).$$

Since $\mathcal{U} = \bigoplus_{i=1}^t \bar{\mathcal{U}}_i$ we conclude that

$$\begin{aligned} d(\mathcal{C}) &= 2k - 2 \max_{j \in \mathbb{N}} \dim(\mathcal{U} \cap \mathcal{U}M^j) \\ &\geq 2k - 2 \sum_{i=1}^t \max_{j \in \mathbb{N}} \dim(\text{rowsp}(\bar{U}_i) \cap \text{rowsp}(\bar{U}_i M_{p_i^{e_i}}^j)) \end{aligned}$$

The cardinality of \mathcal{C} is a direct consequence of the fact that

$$\text{diag}(M_{p_1^{e_1}}, \dots, M_{p_t^{e_t}})^i = \text{diag}(M_{p_1^{e_1}}^i, \dots, M_{p_t^{e_t}}^i)$$

and of the minimality of the least common multiple. ■

It is possible to find examples for which the lower bound given by (2) is attained. The following lemmas depict these examples.

Lemma 20: Let $M := \text{diag}(M_{p_1^{e_1}}, \dots, M_{p_t^{e_t}}) \in GL_n(\mathbb{F}_q)$ a matrix such that $p_i \in \mathbb{F}_q[x]$ are monic irreducible polynomials and $d_i := \deg(p_i^{e_i})$ for $i = 1, \dots, t$. Let $k \leq d_i$ for $i = 1, \dots, t$ and $\mathcal{U} := \text{rowsp}(U_1, \dots, U_t) \in \mathcal{G}_{\mathbb{F}_q}(k, n)$ where $U_i \in \mathbb{F}_q^{k \times d_i}$ are matrices having full rank for $i = 1, \dots, t$. If we define $\mathcal{C} := \{\mathcal{U}M^i \mid i \in \mathbb{N}\}$ and $\mathcal{C}_i := \{\text{rowsp}(U_i)M_{p_i^{e_i}}^j \mid j \in \mathbb{N}\}$ and it holds $\gcd(|\mathcal{C}_i|, |\mathcal{C}_j|) = 1$ for all $i \neq j$, then

$$d(\mathcal{C}) = \min_{i \in \{1, \dots, t\}} d(\mathcal{C}_i).$$

Proof: We only need to show that there exists a codeword of \mathcal{C} that satisfies this minimum. Up to a permutation of $\{1, \dots, t\}$ we can consider that the code \mathcal{C}_1 is satisfying the minimum distance. Let $g_1 \in \mathbb{N}$ be such that $d(\text{rowsp}(U_1), \text{rowsp}(U_1)M_{p_1^{e_1}}^{g_1}) = d(\mathcal{C}_1)$. Since the cardinalities of the codes \mathcal{C}_i are pairwise coprime, it follows that there exists $g \in \mathbb{N}$ such that

$$g \equiv g_1 \pmod{|\mathcal{C}_1|} \quad \text{and} \quad g \equiv 0 \pmod{|\mathcal{C}_j|}$$

for $j = 2, \dots, m$. We obtain that

$$\begin{aligned} d(\mathcal{U}, \mathcal{U}M^g) &= d(\mathcal{U}, \mathcal{U}\text{diag}(M_{p_1^{e_1}}^{g_1}, I, \dots, I)) \\ &= d(\text{rowsp}(U_1), \text{rowsp}(U_1)M_{p_1^{e_1}}^{g_1}) = d(\mathcal{C}_1) \end{aligned}$$

Lemma 21: Let $M := \text{diag}(M_{p_1^{e_1}}, \dots, M_{p_t^{e_t}}) \in GL_n(\mathbb{F}_q)$ such that $p_i \in \mathbb{F}_q[x]$ are monic irreducible polynomials and $d_i := \deg(p_i^{e_i})$ for $i = 1, \dots, t$. Let $k_i \leq d_i$, $\bar{U}_i \in \mathbb{F}_q^{k_i \times d_i}$ be matrices with full rank and $\mathcal{U} := \text{diag}(\bar{U}_1, \dots, \bar{U}_t) \in \mathcal{G}_{\mathbb{F}_q}(k, n)$. If we define $\mathcal{C} := \{\mathcal{U}M^i \mid i \in \mathbb{N}\}$ and $\mathcal{C}_i := \{\text{rowsp}(\bar{U}_i M_{p_i^{e_i}}^j) \mid j \in \mathbb{N}\}$ and it holds $\gcd(|\mathcal{C}_i|, |\mathcal{C}_j|) = 1$ for all $i \neq j$, then

$$d(\mathcal{C}) = 2k - 2 \sum_{i=1}^t \max_{j \in \mathbb{N}} \dim(\text{rowsp}(\bar{U}_i) \cap \text{rowsp}(\bar{U}_i M_{p_i^{e_i}}^j)).$$

Proof: Also here we show a codeword of \mathcal{C} which satisfies the relation. Let $g_1, \dots, g_t \in \mathbb{N}$ be such that $\dim(\text{rowsp}(\bar{U}_j) \cap \text{rowsp}(\bar{U}_j M_{p_j^{e_j}}^{g_j}))$ is maximal for $j = 1, \dots, m$. Since the cardinalities of the codes are pairwise coprime, it follows that there exists a $g \in \mathbb{N}$ such that

$$g \equiv g_j \pmod{|\mathcal{C}_j|}$$

for any $j = 1, \dots, t$. Then,

$$\begin{aligned} d_{\min}(\mathcal{C}) &= d(\mathcal{U}, \mathcal{U}\text{diag}(M_{p_1^{e_1}}^{g_1}, \dots, M_{p_m^{e_m}}^{g_m})^g) \\ &= d(\mathcal{U}, \mathcal{U}\text{diag}(M_{p_1^{e_1}}^{g_1}, \dots, M_{p_m^{e_m}}^{g_m})) \end{aligned}$$

$$= 2k - 2 \sum_{j=1}^m \dim(\text{rowsp}(\bar{U}_j) \cap \text{rowsp}(\bar{U}_j M_{p_j^{e_j}}^{g_j})).$$

A matrix $M \in GL_n(\mathbb{F}_q)$ is called completely reducible if its elementary divisors are all irreducible, i.e., from Definition 5 if $e_{i,j} = 1$ for all i, j . One can use the theory of irreducible cyclic orbit codes from [9] to compute the minimum distances of the block component codes in the extension field representation and hence with Theorem 19 a lower bound for the minimum distance of the whole code. ■

CONCLUSIONS

Due to the characterization of conjugacy classes of cyclic subgroups of $GL_n(\mathbb{F}_q)$, we were able to conclude that every cyclic orbit code is conjugated to a cyclic orbit code defined by the cyclic group generated by a matrix in rational canonical form. The research of orbit codes with good parameters can then be restricted to this subclass of cyclic orbit codes.

The following step in this research direction is to completely classify orbit codes. In order to do so we have to find a characterization of the conjugacy classes of subgroups of $GL_n(\mathbb{F}_q)$ that possibly coincides with the one presented in Section I if restricted to cyclic subgroups of $GL_n(\mathbb{F}_q)$.

REFERENCES

- [1] R. Kötter and F. Kschischang, "Coding for errors and erasures in random network coding," *Information Theory, IEEE Transactions on*, vol. 54, no. 8, pp. 3579–3591, August 2008.
- [2] F. Manganiello, E. Gorla, and J. Rosenthal, "Spread codes and spread decoding in network coding," in *Proceedings of the 2008 IEEE International Symposium on Information Theory*, Toronto, Canada, 2008, pp. 851–855.
- [3] A. Kohnert and S. Kurz, "Construction of large constant dimension codes with a prescribed minimum distance," in *MMICS*, ser. Lecture Notes in Computer Science, J. Calmet, W. Geiselmann, and J. Müller-Quade, Eds., vol. 5393. Springer, 2008, pp. 31–42.
- [4] T. Etzion and N. Silberstein, "Error-correcting codes in projective spaces via rank-metric codes and ferrers diagrams," *Information Theory, IEEE Transactions on*, vol. 55, no. 7, pp. 2909–2919, jul. 2009.
- [5] V. Skachek, "Recursive code construction for random networks," *Information Theory, IEEE Transactions on*, vol. 56, no. 3, pp. 1378–1382, March 2010.
- [6] A.-L. Trautmann, F. Manganiello, and J. Rosenthal, "Orbit codes - a new concept in the area of network coding," in *Information Theory Workshop (ITW), 2010 IEEE*, Dublin, Ireland, Aug. 2010, pp. 1–4.
- [7] I. N. Herstein, *Topics in Algebra*, 2nd ed. Lexington, Mass.: Xerox College Publishing, 1975.
- [8] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and their Applications*. Cambridge, London: Cambridge University Press, 1994, revised edition.
- [9] A.-L. Trautmann and J. Rosenthal, "A complete characterization of irreducible cyclic orbit codes," in *Proceedings of the Seventh International Workshop on Coding and Cryptography (WCC) 2011*, 2011, pp. 219–223.